

# Dataskyddspolicy

**Dokumentägare:** Chefsjurist

**Skapad:** 2018-05-23

AcadeMedia behandlar en stor mängd personuppgifter varje dag. Detta är nödvändigt för att vi ska kunna utföra vårt uppdrag på ett effektivt och rättssäkert sätt. Det är viktigt att all sådan behandling genomförs korrekt och inte riskerar att göra intrång i den personliga integriteten hos de individer vars personuppgifter vi behandlar, exempelvis våra medarbetare, barn, elever och deltagare. Om personuppgifter som vi har samlat in nyttjas i andra syften än vad som är tänkt, behandlas på ett otillbörligt sätt, eller om de hamnar i fel händer, kan det leda till allvarlig skada för enskildas personliga integritet. Många av uppgifterna tillhör barn, vars uppgifter förtjänar särskilt skydd.

Det är en viktig fråga för AcadeMedia att skydda den personliga integriteten för våra barn, elever, vårdnadshavare, vuxna deltagare och medarbetare. Det betyder att vi som arbetar på AcadeMedia måste hantera uppgifter på ett tryggt och ansvarsfullt sätt.

Syftet med denna policy är att tydliggöra hur AcadeMedias medarbetare ska agera för att säkerställa att våra deltagares, vårdnadshavares och medarbetares integritet respekteras och att all personuppgiftsbehandling sker i enlighet med dataskyddsförordningen och annan tillämplig dataskyddslagstiftning. Policyn innehåller information om (i) ansvarsfördelningen för dessa frågor inom AcadeMedia-koncernen, (ii) dataskyddsförordningens syfte och viktiga begrepp, (iii) fördjupad beskrivning av vad som är en personuppgift samt (iv) vad vi på AcadeMedia generellt måste tänka på när vi behandlar personuppgifter.

## AcadeMedias organisation för personuppgiftshantering

Inom AcadeMedia gäller att personuppgiftsansvaret ligger på den verksamhet som styr över behandlingen av personuppgifter avseende barn, elever, vårdnadshavare, vuxna deltagare samt externa kunder och kontakter. Det betyder till exempel att Vittraskolorna AB har det yttersta ansvaret för den personuppgiftsbehandling som sker på Vittras förskole- och skolenheter. AcadeMedia Support AB är personuppgiftsansvarig för personuppgiftsbehandling av samtliga medarbetare i Sverige. AcadeMedias verksamheter utanför Sverige är personuppgiftsansvariga för all behandling av personuppgifter i det landet, inklusive uppgifter om medarbetare.

Varje segment inom AcadeMedia ska säkerställa att det finns konkreta riktlinjer för tillämpningen av denna policy och att alla medarbetare följer och ges kunskap om riktlinjerna och tillhörande rutiner. Segmenten ansvarar även för att all personal genomgår koncernens webbutbildning i dataskydd och i övrigt ger medarbetarna tillräcklig kompetens och förutsättningar att uppfylla dataskyddsförordningen.

Respektive segment ska säkerställa att ingående verksamheter har minst ett dataskyddsombud som har det operativa tillsynsansvaret för segmentets personuppgiftshantering samt ansvar för att uppdatera segmentets förteckning över personuppgiftsbehandling.

Information om dataskydd finns samlad på AcadeMedias svenska webb. Där finns också policies, riktlinjer och mallar som kan behövas vid hantering av personuppgiftsfrågor.



## Dataskyddsförordningen

Dataskyddsförordningen, eller GDPR, gäller från och med den 25 maj 2018 som lag inom EU och därmed Sverige och ersätter då den tidigare personuppgiftslagen (PuL). Dataskyddsförordningen syftar till att skydda människors personliga integritet när personuppgifter behandlas.

Dataskyddsförordningen gäller för både manuell och elektronisk hantering av uppgifter, så länge som uppgifterna är sökbara.

## Viktiga begrepp

### Personuppgifter

Personuppgifter är all slags information som, direkt eller indirekt, kan knytas till en fysisk person som är i livet.

### Personuppgiftsbehandling

Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

### Personuppgiftsansvarig

Den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter (det vill säga varför och hur personuppgifter ska behandlas).

Personuppgiftsansvarig är nästan alltid en [juridisk person](#), ett företag eller en organisation.

### Dataskyddsombud

En fysisk person som, efter att ha utsetts av den personuppgiftsansvarige, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

### Personuppgiftsbiträde

En fysisk- eller juridisk person, utanför den egna personuppgiftsansvariga organisationen, som behandlar personuppgifter för den personuppgiftsansvariges räkning.

## Vad är en personuppgift?

Personuppgifter är, som nämnts ovan, all slags information som, direkt eller indirekt, kan knytas till en fysisk person som är i livet. Personuppgifter kan därför vara allt ifrån uppgifter om namn och adress till betyg, frånvaro, hemförhållanden, löner, foton eller ljudinspelningar. En utgångspunkt för AcadeMedias dataskydd är att personuppgifterna tillhör den enskilde, vi lånar dem bara.

Alla personuppgifter ska behandlas med lämplig säkerhet och respekt. Ju känsligare personuppgifterna är ur ett integritetsperspektiv, desto högre krav ställs på skydd och säkerhet. Vid behandling av personuppgifter ska vi därför kontinuerligt fundera över och bedöma hur integritetskänsliga uppgifterna är och anpassa säkerheten därefter. För detta syfte kan vi därför dela in personuppgifterna i följande 3 kategorier:

### 1. Okänsliga personuppgifter

Normalt sett är uppgifter om namn, adress, betyg, förskola, arbetsgivare och kundförhållanden harmlösa personuppgifter.

### 2. Känsliga personuppgifter



# AcademeMedia

Känsliga personuppgifter utgör en särskild kategori i dataskyddsförordningen och ska behandlas med särskild varsamhet. Känsliga personuppgifter definieras som personuppgifter som avslöjar uppgift om följande:

1. ras eller etniskt ursprung
2. politiska åsikter
3. religiösa eller filosofiska uppfattningar
4. fackligt medlemskap
5. genetiska uppgifter
6. biometriska uppgifter
7. hälsa
8. sexualliv
9. sexuell läggning

### 3. Integritetskänsliga personuppgifter

Det finns ett antal personuppgifter som inte nödvändigtvis träffas av dataskyddsförordningens definition av känsliga personuppgifter ovan, men som fortfarande är integritetskänsliga. Det kan exempelvis avse uppgifter om personnummer, hemförhållanden, ekonomi, beteendeproblematik och kränkande behandling. Sådana uppgifter ska likt känsliga personuppgifter behandlas med extra varsamhet och bara om det är nödvändigt.

## Vad krävs vid behandling av personuppgifter?

Dataskyddsförordningen ställer krav på bland annat hur, var, när, hur länge och av vem personuppgifter får behandlas. Nedan anges de centrala delar som vi måste tänka på när vi behandlar personuppgifter.

### Rättslig grund

Vi måste ha stöd i dataskyddsförordningen för att hantera personuppgifter. Så länge vi behandlar uppgifter för att utföra vårt uppdrag enligt skollagen kan vi hänvisa till den rättsliga grunden att vi utför uppgift av **allmänt intresse** eller som ett led i vår **myndighetsutövning**.

Andra rättsliga grunder relevanta för personuppgiftsbehandling i vår verksamhet är:

- **Rättslig förpliktelse.** Vi är till exempel skyldiga att behandla personuppgifter för att uppfylla bokföringsskyldigheten i bokföringslagen eller för att fullgöra våra skyldigheter enligt kollektivavtal.
- **Avtal.** För att fullgöra eller ingå exempelvis anställningsavtal, kundavtal och leverantörsavtal måste vi behandla personuppgifter (men bara de uppgifter som behövs för att uppfylla avtalet).
- **Intresseavvägning.** Det är också möjligt att hantera personuppgifter efter en så kallad intresseavvägning om vi kan visa att vårt intresse av att hantera uppgifterna väger tyngre än den enskildes rätt till personlig integritet. I många fall kan vi använda intresseavvägning som grund för att hantera personuppgifter vid marknadsföring och direktreklam.
- **Samtycke.** Ett annat alternativ är att be personen ifråga att få behandla uppgifter om honom/henne. Det kallas för att få personens samtycke. Ett samtycke måste vara en frivillig



# AcadeMedia

och tydlig viljeytring, genom vilken den registrerade godtar behandling av personuppgifter som rör honom eller henne. Personen måste få tydlig information om vilka uppgifter som samlas in och vad de ska användas till, för att man ska kunna ge sitt godkännande. Vi måste genom skriftlig dokumentation kunna visa att vi fått ett samtycke. Vi använder bara samtycke när ingen av de ovan nämnda rättsliga grunderna är tillämpliga.

*Särskilt om rättslig grund vid behandling av känsliga personuppgifter.* Huvudregeln i dataskyddsförordningen är att behandling av känsliga personuppgifter är förbjuden. Det finns dock undantag till denna huvudregel. Känsliga personuppgifter får behandlas om det finns särskild rättslig grund för sådan behandling. De rättsliga grunderna för behandling av känsliga personuppgifter är något färre och strängare jämfört med de för andra personuppgifter.

I vår verksamhet behandlas en omfattande mängd känsliga personuppgifter, exempelvis inom ramen för elevhälsan och vid hantering av stödbehov och allergier. Den rättsliga grunden för vår behandling av känsliga personuppgifter kan, i de flesta fall, stödjas på den rättsliga grunden att det är nödvändigt av hänsyn till ett viktigt *allmänt intresse*.

## **Informera**

När vi samlar in uppgifter om en person måste vi informera den berörda personen och/eller vårdnadshavare om hur deras eller deras barns personuppgifter behandlas. Den information som måste lämnas är, bland annat, vem som är personuppgiftsansvarig, vilka personuppgifter som samlas in, rättslig grund för behandlingen, vad uppgifterna ska användas till, hur länge uppgifterna ska sparas, var personen kan vända sig med klagomål samt att denne har rätt att exempelvis få tillgång till sina personuppgifter och begära rättelse av felaktiga uppgifter. All information ska finnas samlad på [trygg.academedia.se](http://trygg.academedia.se), respektive personuppgiftsansvarig inom AcadeMedia svarar för att hålla sin information uppdaterad.

## **Samla bara in de uppgifter som behövs för ändamålet**

Personuppgifter får inte samlas in bara för att de är bra att ha. Vi måste säkerställa att de uppgifter som vi vill samla in är nödvändiga för ändamålet med behandlingen.

## **Använd enbart uppgifterna till det som beskrivits vid insamlandet**

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Det betyder att uppgifter som samlas in för ett visst syfte, inte sedan får användas för helt andra syften. Vi kan alltså inte samla in elevuppgifter för att föra ett register över utlånade datorer och sedan använda uppgifterna för att marknadsföra våra andra skolor.

## **Se till att uppgifterna är korrekta**

Personuppgifterna som vi registrerar ska vara korrekta och uppdaterade. Den som behandlar personuppgifter ska därför vidta alla rimliga åtgärder för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål. Det innebär att om en elev hör av sig till skolan och meddelar att elevens adress är felaktig i våra system är skolan skyldig att rätta uppgiften.

## **Spara så kort tid som möjligt**

Vi får inte spara personuppgifter för längre tid än vad som behövs för ändamålet. När de inte längre behövs för det syfte som de en gång samlades in för, ska de tas bort. För oss betyder det exempelvis att uppgifter om elever eller deltagare som inte längre går på våra skolor ska tas bort från IT-system och andra platser där de sparats. I vissa fall behöver vi dock spara uppgifterna längre än så, exempelvis när det följer av lag eller om det av annan anledning är nödvändigt att spara dem.

Se AcadeMedias [arkiveringsplan](#) för information om vilka uppgifter som ska sparas och hur länge.

## **Enskilda rättigheter**



# AcadeMedia

Enligt dataskyddsförordningen har de personer, vars personuppgifter vi behandlar, vissa rättigheter. De har exempelvis rätt att få tillgång till sina personuppgifter och även att få sina personuppgifter raderade eller rättade. Alla förfrågningar från en registrerad om att utnyttja dessa rättigheter ska kanaliseras via verksamhetens dataskyddsombud. Vid osäkerhet kring hantering ska dataskyddsombudet alltid ta kontakt med Juridik och/eller IT.

## Säkerhet

Alla personuppgifter inom AcadeMedia ska hanteras med lämpliga säkerhetsåtgärder som är anpassade utifrån uppgifternas känslighet. Inom AcadeMedia använder vi därför bland annat följande säkerhetsåtgärder:

- Behörighetsstyrning. Bara de som har behov av uppgifter får behandla dem..
- Krypteringsskydd. Epost inom AcadeMedia är krypterad när den sänds över internet och det finns därutöver möjlighet att lösenordsskydda en fil, vilket normalt sett innebär att även innehållet krypteras. Vår molnbaserade lagring (Google och OneDrive) lagras krypterat i molnet.
- Delningsplattformar. Istället för att mejla en fil kan man dela ett dokument som lagras i en molntjänst (till exempel Google Drive) vilket innebär att man kan styra tillgången till informationen även i efterhand.
- Stark autentisering. Valda tjänster inom vår IT-miljö kan få stark autentisering, exempelvis engångslösenord eller BankID.
- Anonymisering och maskning. Data som presenteras i många av våra system kan anonymiseras för att undvika att visa uppgifter på en individuell nivå.

## Personuppgiftsincidenter

Om vi låter en extern part behandla personuppgifter för vår räkning, till exempel Schoolsoft eller Benify, ska det alltid tecknas ett avtal som reglerar behandlingen av uppgifterna. I avtalet ska det bland annat stå att leverantören får behandla personuppgifterna bara i enlighet med våra instruktioner och att leverantören är skyldig att upprätthålla god säkerhet. AcadeMedias mall ska användas för de svenska verksamheterna, vid eventuella undantag ska alltid Juridik eller IT involveras.

## Särskilda områden

### Kameraövervakning

Kameraövervakning innebär att personuppgifter behandlas. Allt inspelat videomaterial är att betrakta som integritetskänsliga personuppgifter och måste hanteras som sådant. Kameraövervakning är inte en lösning som ska väljas i första hand. Ofta finns andra sätt att komma åt ordningsproblem och liknande och sådana bör väljas före kameraövervakning.

För att en verksamhet ska få sätta upp övervakningskameror krävs det att det finns ett övervakningsintresse som väger tyngre än integritetsintresset. Det är utbildningens huvudman som ska visa på att det finns ett rättsligt stöd för kameraövervakningen. Läs mer [här](#).

### Skyddade personuppgifter

Se AcadeMedias dokumentation för hantering av skyddade personuppgifter som finns tillgängligt via medarbetarwebben.

- [När medarbetare har skyddade personuppgifter](#)
- [När barn och elever i förskolan och grundskolan har skyddade personuppgifter](#)



# AcadMedia

- [När elever på gymnasiet har skyddade personuppgifter](#)

